Missouri Department of Mental Health

The DMH Outcomes Web

Development Plan

G. Harbison, MA, DMH Outcomes Coordinator

November 2000

Technology is not the hard part… The hard part is what has to be done to take advantage of the technology - Louis Gerstner, CEO of IBM

Contents

The Internet finally gives government the tools it needs to begin to re-engineer the care delivery systems for clients in ways that have been talked about for years.
- Gerald E. Driggs, President of CS & O

DMH Outcomes Web Development Plan

*Business Purpose:

- Meet increased interest in performance measurement and quality improvement.
- Allow maximum flexibility in responding to changing performance measurement and quality improvement needs.
- Establish reliable and practicable data source for performance.
- Ensure ease of data entry and report generation.
- Reduce burden of data collection on providers.
- Maximize data integrity.
- Address the 1996 DMH Strategic Plan: Establish a single system of outcomes and performance measurement.

*Description:

The DMH Outcomes Web is a mechanism for automated collection of outcomes and Performance Measurement data, and timely distribution of informative reports based on the collected data. The DMH Outcomes Web makes use of a Virtual Private Network operating through the public Internet via secure and private connections. The DMH Outcomes Web uses web-based applications for the entry of outcomes data and timely distribution of and access to outcomes and Performance Measurement[1] data and reports.

- Web Based Technology is[2]:

Technical architecture consisting of at least three levels of hardware and software:

1. User interface through a PC with a web browser
2. Communicating with a "web server" that stores, creates, or locates new "pages" for display on the browser.

[1] For additional information on the DMH system of Performance Measurement see: Outcomes and Performance Measurement: Policy, Principles and Operational Guidelines.

[2] Description provided by Office of Information Systems.

3. Data and possibly other programming logic are located on other computers called "database servers" or "application servers"
4. All these computers communicate using the standard internet protocol (TCP/IP)

- Advantages of Web Based Technology:

1. The "web interface" including images, menus, buttons, and "links" is intuitive, easy to learn, and already familiar to many people.
2. Communication can take place over public networks using encryption to maintain privacy, so the application may be accessed from "any" location.
3. The web browser and the encryption software are the only software required on the user's PC, so less support is needed at the user's location.
4. Software revisions are easier to deploy quickly, since only the server software needs to be updated.
5. Web technology is consistent with the DMH Strategic Plan for Information Technology and with market trends.
6. Web applications allow two-way real time communication, instead of batch updates to data on a daily basis, so information is timely.
7. The application can access data from other systems, so data from a new system can be accurately integrated with previous data.

*Features:

- Provider agencies have secured access to client-specific outcomes data (i.e., only their own clients), client-specific reports, agency reports, statewide reports, reports of other Performance Measures, and reports of data integrity.

- Outcomes data is connected to other administrative data, allowing for analysis of additional factors, such as correlation between outcomes and service utilization.

- The system is flexible to meet the data collection and report generation needs of the service Divisions.

- This system can be used to create automated versions of practice guidelines.

- The system will highlight due dates for routine data reporting through prompts.

- Data entry will be accomplished through the same system.

- The system will allow for correction of certain data integrity problems at the provider level.

- Additional data integrity problems will be highlighted through this system and identified for correction through other means.

- Data and reports will also be available to Central Office and to regional offices.
- The system places data at the level closest to the user of the data. This will enhance usefulness of the information and will encourage the continued refinement of the system.

- This system could allow for collection of "early warning" data in the early phases of any large scale changes to the service system in order to ensure success of the operation (i.e., key indicators that could warn of service system failure and that could be collected separately from systems in transition, such as claims entry or encounter data).

- This system will also allow for analysis of the outcomes of individuals served by more than one Division.

*Goals and Objectives:

- The primary goal is to increase the usefulness of any collected data by ease of timely access while meeting the data collection needs of the Divisions.

- All aspects of an outcomes and Performance Measurement system will be more effective, timely and efficient.

- This system will also place an emphasis on data integrity by making weaknesses in reports apparent and by connecting outcomes data to existing administrative data (i.e., CTRAC or CIMOR).

- The nature of the automation (i.e., that it is web technology) will, in and of itself, generate interest and use of the data.

*Market Assessment:

- There are no known systems of this type in use in the public mental health sector, although some commercial managed care companies have made limited, but successful, use of this type of application in commercial mental health services.

- This system should have national application.

- Existing outcomes systems are either paper-based and utilizing a freestanding database or automated with another technology utilizing a freestanding database.
  - Experience with paper-based data collection and report generation indicates several weaknesses, including poor connection to existing data, increasing needs for use of staff resources to deal with system management, oversight and operations, especially in terms of data integrity and timeliness of reports.
  - Systems utilizing some other form of automation have historically had difficulty connecting with existing administrative data. In addition, report distribution (for statewide data) is mostly on paper and requires many staff resources to simply ensure that reports are delivered to providers and other users.

*Consumer/User Profile/Market:

- The need for increased accountability is an area of broad agreement with in the public Mental Health system.

- Literally every DMH system stakeholder is a potential consumer of the products of this system, from individual consumers (for example, report cards on the DMH public web-site) to providers to elected officials to any Missourian interested in use of taxpayer dollars in public mental health services.

- This system will be a model for other states and national initiatives since accountability is paramount in mental health services and since no one has made use of web technology to meet these challenges.

- The primary market consists of the many providers of ADA, CPS and MRDD services located throughout the state.

- Another important market is the DMH system itself, including administration, service Divisions, Regional Administrators, Licensure and Certification and other sections of the Office of Quality Management.

- The use of this system is limited only by the amount and type of data collected and the sophistication and speed with which informative reports can be produced.

*Marketing Plan:

Meeting Customer Needs:

- The public mental health system in Missouri is hungry for useful and easily accessed data that addresses service quality and performance and facilitates the improvement of services.
- This product will make all aspects of performance measurement and reporting easier, quicker and more useful than anything previously available.
- Provider and consumer support is essential.
- The flexibility of the technology will make it easier to exceed customer expectations, and to change as those needs change.

Delivery:

- Web-based applications require only that the user has access to our web system, has current software to read WebPages (a web browser), and encryption software.
- DMH will need to develop a protocol for the assignment of provider passwords for security purposes (similar to that in use with MSAS[3]) and encryption software will be installed on user computers. In addition, other aspects of security will require attention, such as electronic certificates and secure firewalls.
- Provider training will be conducted to facilitate use and operation of the system.

[3] Missouri Service Authorization System: A web –based application designed by the DMH Office of Information Systems and ADA for authorization of Comprehensive Substance Treatment and Rehabilitation (CSTAR).

*Operations:

Management Team:

- Outcomes Coordinator
- OIS Representatives
- Division Representatives
- This group has varied experience with performance measurement initiatives.
- Strength exists in encountering the same issues in each division.
- Each division has had some success with performance measurement.
- The Performance Measurement Group will be used to coordinate system operations[4].

Human Resources:

- The system will require partial support from the following staff:
  - Outcomes Coordinator, Office of Quality Management
  - Research Analyst III, OQM
  - Research Analyst II, OQM
  - Deputy Director, CPS
  - Deputy Director, ADA
  - Deputy Director, MRDD
  - Deputy Director, OIS
  - Web Development staff, OIS
- Assessment of future human resource needs: System will require expansion of staff support as modules are added. However, as each section is brought on-line and established, staff support will be reduced to a standard level less than required at start-up for each section.

[4] The Performance Measurement Group (PMG) has been established to ensure input and shared resources, and to facilitate coordination. The charge of the Performance Measurement Group is to assist the Outcomes Coordinator in the formulation, implementation, monitoring and refinement of Performance Measures that indicate the quality of Department operations and that support system improvement and management. In addition, the PMG recommends performance standards for specific measures. The PMG represents all areas of DMH. The Outcomes Coordinator chairs the PMG. Current membership includes Gary Harbison (chair), Rosie Anderson-Harper, Karen Battjes, Janet Conboy, Mildred Glasper, Mary Kay Gratz, Rhonda Haake, Patti Killingsworth, Gary Lyndaker, Bob McClain, Wallace McMullen, Steve Reeves, Judy Rizner and Allen Templeton.

*Components:

Outcomes Components:

Populations/Services:

- ADA: CSTAR and GTS Adults
- CPS: CPRC, TCM Adults and Children
- MRDD: Family Directed Supports
- Other Populations/Services as requested/needed

Operational Components[5]:

- Active Agency Client Listing (connection to CTRAC)
- Outcomes and Performance Data Entry
- Individual Client Reports
- Agency Reports
- State-Wide Reports
- Data Integrity Reports
- Custom Queries
- Download of Agency Data

*Developmental and Technical Considerations:

- Major Technical equipment to support this project includes[6]:
  - Web Server
  - VPN Concentrator
  - PIX Firewall
  - Security Certification Software
  - Server for CTRAC Connection
  - Encryption Software

- Security
  - This system will meet or exceed Health Care Financing Administration Policy of electronic transmission of data[7].

[5] See Diagram 1: Outcomes Web Operations.

[6] See Diagram 2: Outcomes Web/Virtual Private Network Technology.

- Technical Support
  - Consultation time will be required to properly design and activate this system.

- Bandwidth Limitations:
  - Some areas of the state may lack the telecommunication lines and equipment to efficiently support the transfer of large amounts of data. Only pilot testing will determine limitations.
  - The existing dial-up network will be available for limited use at provider discretion.

- Network Capacity:
  - Connectivity through current CTRAC provider connections is limited by system capacity. In addition, the existing dial-up network is no longer matching the required capacity of the existing system.
  - Connectivity through the Internet requires a security protocol and use of server site outside of DMH firewall.

- Data entry at the provider location solves many of the downsides to paper-based data entry and batched data entry (i.e., poor data integrity and poor connection to other data files). However, this may require greater network capacity.

*Recommendations[8]:

- Develop the system in an incremental manner:

  - Phase I: Purchase of hardware and software
    - Use technology consultants for planning and set-up
    - Purchase recommended hardware and software April – June 2000
      - Purchases funded by the Office of the Outcomes Coordinator, the Division of Alcohol and Drug Abuse, the Division of Comprehensive Psychiatric Services, and the Division of Mental Retardation and Developmental Disabilities

---

[7] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) calls for stringent security protection for electronic health information while maintained and while in transmission.

[8] Recommendations developed through the Outcomes Web Development Group: Gary Harbison, Chair, Gary Lyndaker, Peter Wieberg, Bob McClain, Gart Pollard, Patti Killingsworth, Steve Reeves, Karen Battjes, Mary Kay Gratz, Judy Rizner, Wallace McMullen, and Marilyn Gerrard-Hartman. The charge of this group was to determine the practical use of web-based technology in the collection and dissemination of outcomes and other new performance measurements, and to determine a course of action for development of the Outcomes Web.

    - Ongoing operational support provided by the Office of Information Systems

- Phase II: Pilot testing of data collection and report generation
    - OASIS[9] project will be pilot product
    - Conversion of software to web application (MIMH and consultant)
    - Development of automated report generation
    - Pilot to start with 8 – 10 ADA providers in late 2000/early 2001

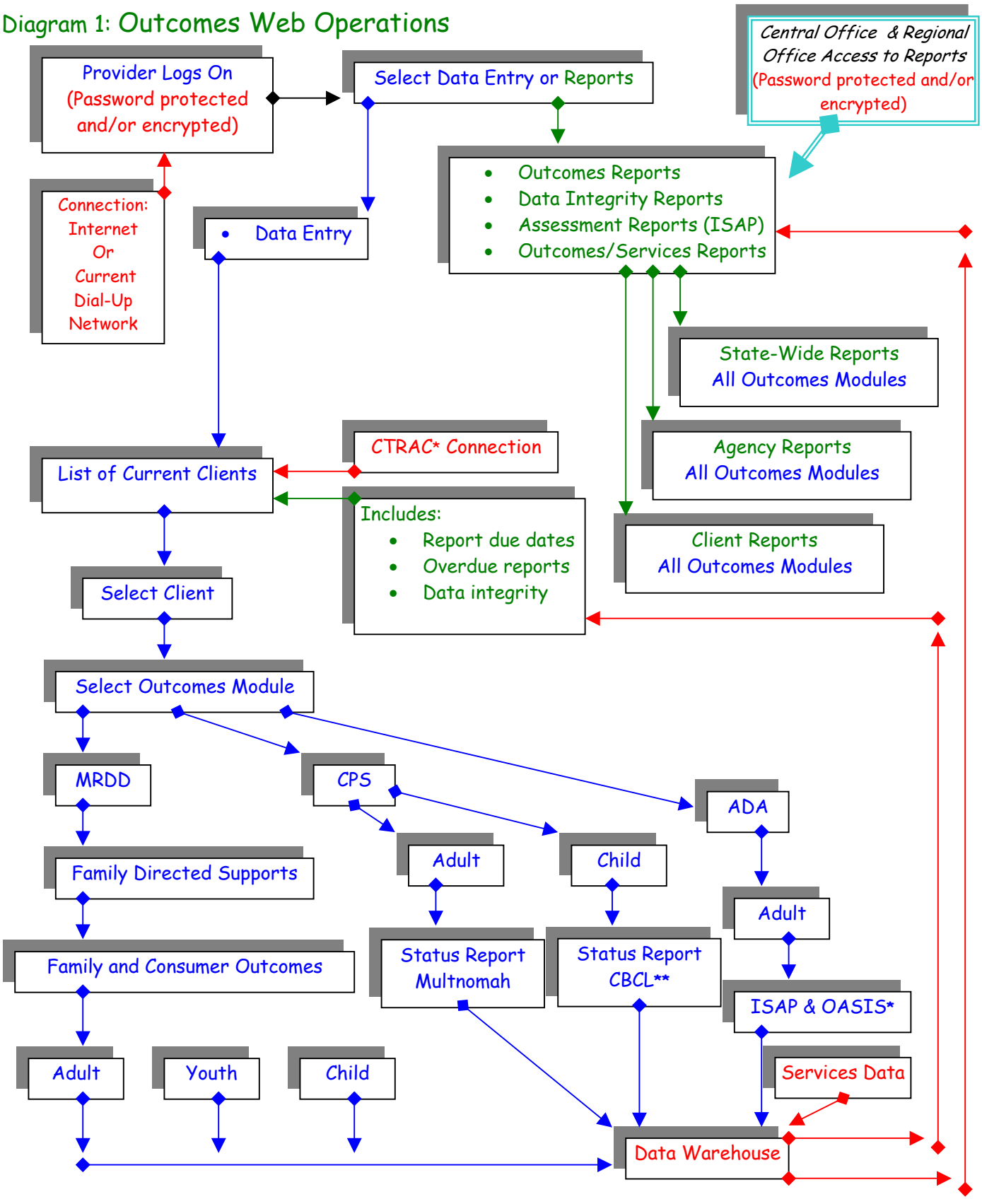
- Phase III: Statewide expansion of OASIS through the Outcomes Web
    - Early – mid 2001

- Phase IV: Expansion to CPS and MRDD and ADA's SATOP
    - Development of Data Entry Software and Piloting: Spring/Summer 2001
    - Development of Report Generation and Electronic Distribution via the Outcomes Web
    - Expansion to statewide application: Fall 2001

- Phase V: Generation of Reports Analyzing Service Utilization and Outcomes
    - Spring 2002

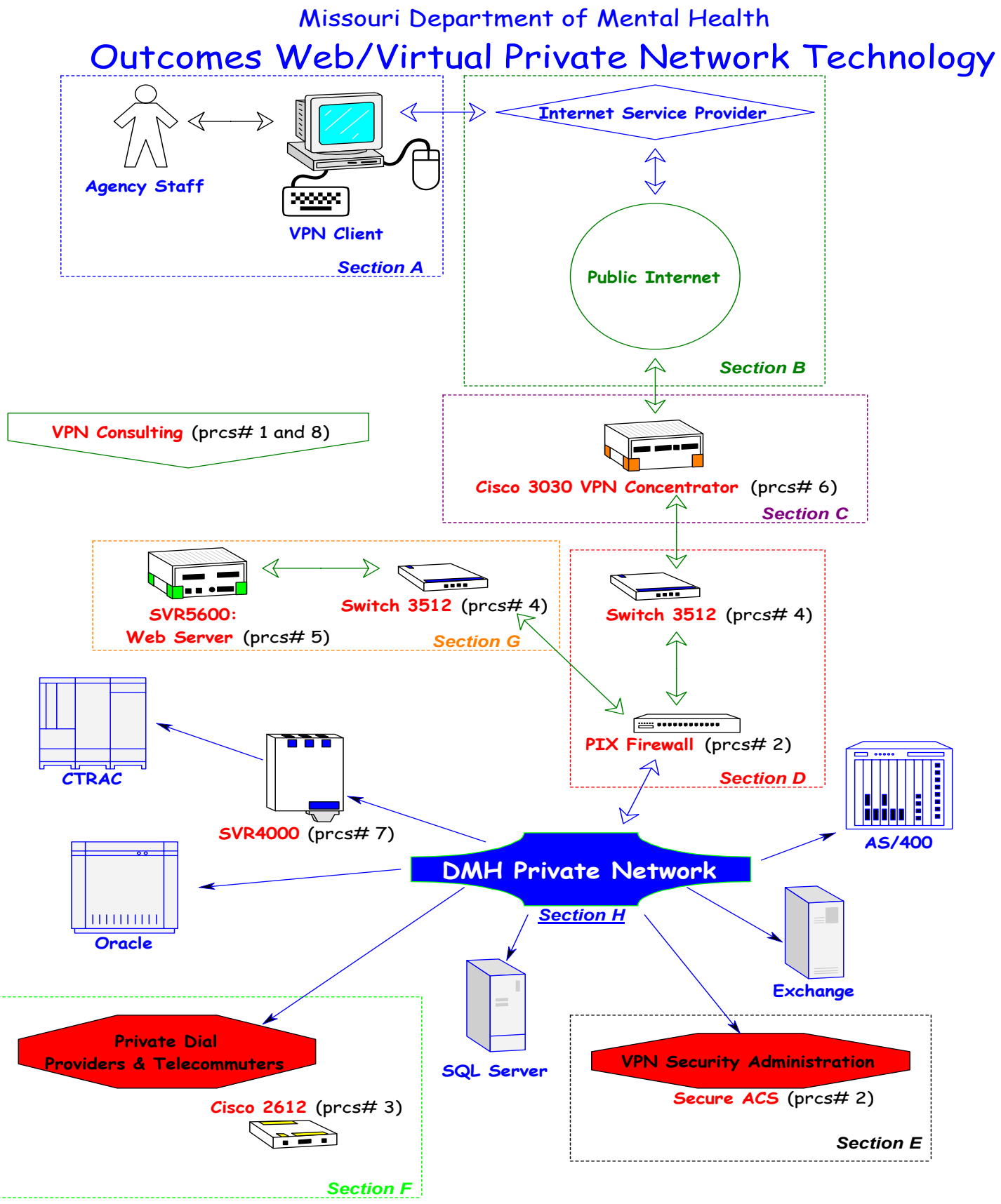
[9] ADA's Outcomes Assessment and Service Improvement System.

Diagram 1: Outcomes Web Operations



* Individual Standardized Assessment Protocol/Outcomes Assessment & Services Improvement System
**Child Behavior Check List
*Client Tracking, Registration, Admissions and Commitments

Diagram 2:


Missouri Department of Mental Health
Outcomes Web/Virtual Private Network Technology
Agency Staff
VPN Client
Section A
Internet Service Provider
Public Internet
Section B
VPN Consulting (prcs# 1 and 8)
Cisco 3030 VPN Concentrator (prcs# 6)
Section C
SVR5600:
Web Server (prcs# 5)
Switch 3512 (prcs# 4)
Section G
Switch 3512 (prcs# 4)
PIX Firewall (prcs# 2)
Section D
CTRAC
SVR4000 (prcs# 7)
AS/400
Oracle
DMH Private Network
Section H
Exchange
SQL Server
Private Dial
Providers & Telecommuters
Cisco 2612 (prcs# 3)
Section F
VPN Security Administration
Secure ACS (prcs# 2)
Section E

Outcomes Web/Virtual Private Network Technology Diagram
- Pete Wieberg, Office of Information Services

Section A – The end-user perspective

Hardware Requirements:

Since the VPN tunnel requires encryption, a mid-size Pentium computer with sufficient memory for the required applications is a must. See below for the section on Internet connectivity, as the hardware requirements will vary by connection method.

Software Requirements:

The following software would be required, unless otherwise noted:

Operating System:	Windows 95, 98, or NT with current service packs
Browser:	Internet Explorer 5.0 with current security patches
VPN Software:	VPN client software provided by DMH

The following software would be optional, unless otherwise noted:

Personal Firewall:	Depending on the type of Internet connection and the provider's network structure
Mainframe Emulator:	Attachmate 6.5 or latest for CTRAC connectivity, if needed
Others:	Software to access appropriate application or host (e.g., Outlook, Client Access, etc.)

Internet Connection:

There are several types of Internet connections available to the end user from local ISP's (Internet Service Providers):

Dial-up	The most common, but slowest, usually allows unlimited access for a fixed cost on a monthly basis, although some service providers now charge for unlimited access, and some have specified lengths of time you can be connected during a single session. A personal firewall would probably be recommended for this type of connection.
ISDN	Similar to dial-up, but uses digital technology and has a higher connection speed than regular dial-up lines. A personal firewall would probably be recommended for this type of connection.
Cable Modem	A full-time connection with high speeds, this brings about some security issues related to the full-time issue, as your computer is constantly exposed to the Internet. This access runs through your cable company line. The personal firewall software would be a requirement in this situation.
ADSL	Similar to Cable Modem, except runs through special phone lines

Dedicated line – no firewall

The computers of a provider are networked together, and have a full-time connection to the internet through a digital phone service. Once again, there is a constant exposure and the personal firewall would be needed on each computer.

Dedicated line – company has a firewall

The computers of a company are networked together, but there is a firewall where the company network connects to the Internet. The personal firewall would not be needed in this case.

Responsibilities/Liabilities:

Doing business on the public Internet carries inherent risks and responsibilities. As a contracted provider or employee, the end user carries the responsibility of ensuring the privacy of client information. With VPN technologies, the connection between the end-user and DMH is encrypted at a level exceeding current federal mandates. Although a low probability risk, hackers can use a "back-door" approach to tap into the end-user's workstation and access DMH information through the encrypted session. This is the primary reason for the personal firewall software being recommended as a standard.

Section B – The Public Internet and Internet Service Providers

The public Internet is a wide open, worldwide network. Many companies are using it to attain huge cost savings and connectivity not possible before the introduction of VPN technologies.

Internet Service Providers sell end-user access into this huge network. They do so with a wide variety of service offerings, restrictions, and pricing. Often, the monthly charge relates directly to the level and quality of service you can expect from the service provider (e.g., cheap access may equal cheap service, poor connection rates, poor connection speeds). You'll want to be aware of time restrictions, available connection speeds, and expected connection rates (non-busy) when looking at potential service providers. It's an extremely competitive business.

This aspect will probably keep some providers away from the VPN process, as the inability to find a reliable ISP would pose a substantial risk during peak business periods (i.e., billing and reporting) of the month.

Another interesting aspect of using the public Internet is that the ISP now becomes a part of the troubleshooting process, albeit a reluctant one. Very little assistance can be expected from the ISP, unless problem replication can clearly pinpoint the problem to the ISP's equipment or service. To overcome this, you can enter into ISP agreements that will guarantee a given level of service (for a given price, of course).

From a disaster recovery planning point, a private-dial backup plan must be available for a minimum number of end-users utilizing the VPN structure.

Section C – The VPN Concentrator – where the end-user enters DMH

While the end-user supplies hardware and software to create one end of the tunnel, DMH must provide the hardware and software to provide the other end, which becomes the entry point of the end-user's encrypted tunnel into the DMH private network.

The VPN Concentrator accepts properly authorized sessions from the end-users, and allows them access to the appropriate (per end-user) DMH resources. The interaction with a common security administration (see section E) process is critical.

For disaster recovery purposes, there should be multiple VPN Concentrators located around the state, using different Internet Service Providers as the connection into the public Internet. For example, the VPN Concentrator in Jefferson City will be connected to MoreNet, the University of Missouri's public Internet service. Additional VPN Concentrators would be located in St. Louis, Kansas City, and potentially other metropolitan areas and primary and/or secondary access points in case of failure in the Jefferson City area. These additional points would then be connected to other Internet Service Providers, such as AT&T, to reduce the aspect of single points of failure.

Technical note: address IP pooling, DHCP, automated client setup,
Pre-shared encryption keys, RADIUS connectivity,
User/Group controls, 3DES levels, monitoring software

Section D – Firewalling – the 2nd line of defense

Once the end-user enters into the DMH network, we still wish to limit further where they can go, and what they can access with the extended filtering capabilities of a firewall. This would permit explicit services to the outside users coming in, but allow full access (if needed) and device management to internal DMH staff.

The security structure should ensure that (a) the end-user can access the specific web applications available to them; (b) the web server can connect to internal data sources for the appropriate information; and (c) there is no direct connection allowing the end-user to bypass and go directly to the data sources. All application functions related to non-DMH entities should be proxied in some manner for maximum security purposes.

Some of these same services could be accomplished at the VPN Concentrator itself, but in order to avoid duplicate effort related to multiple VPN concentrators (future), it is best handled at the firewall.

In this design, the firewall is currently the most critical single point of failure, and building redundancy must be addressed as a short-term strategy.

Section E – Security Administration of all entry points

A redundant security administration setup must be available to (a) authenticate users as they enter the fringes of the DMH network, (b) log their connection to the network, and (c) apply the appropriate access restrictions (host, application, time period, etc.).

A flexible security administration would be able to handle these functions regardless if the end-user enters through the VPN process or through the private dial-up network. This security administration tool could also be used to control other access within DMH, such as access to the internet via the DMH firewall.

If required by future needs, this tool could also utilize 3rd factor security elements, such as smart cards, etc. to enhance validation of the end-user.

From a total security setup, the logging of all session activity entering DMH at the fringes is a critical element. The security administration tool must meet this mandate.

Section F – Private dial-up users

Since it's doubtful that all DMH providers and telecommuters have the technical capabilities to utilize the VPN structure, replacing our existing dial-up network with newer technology is a must.

The newer technology must support better connection speeds, while working with the security administration tools (section E) to ensure better control and logging of all users entering the DMH network at a fringe access point.

The new DMH "private dial" network will be considerably more limited than the current model, as long-distance calling rates can now be used in place of distributed equipment locations, reducing the need for more extensive equipment maintenance, and allowing better utilization of equipment resources due to larger pooled dial-in locations.

One issue to remember is that at some point, all dial-up access, not just over the Internet, may require encryption technologies to meet state and/or federal mandates. The providers unable to meet the technology structures in the short term may be forced there in the longer timeframe (2-3 years) regardless.

Section G – Web Outcomes and other web-enabled services

Once the end-users enter the DMH network, we need to provide services to them of business interest, such as Outcomes, CTRAC, POS, MSAS, or other information. The VPN structure deals with access to information that is considered covered under the privacy rules and regulations.

Information that is public in nature (non-confidential) can be delivered through the VPN process, but is usually delivered at a different point in the network, accessible to the public Internet, but without the extensive security overhead of the VPN structure.

Section H – Services available on the DMH network to the remote users

For DMH staff (e.g., auditors, case managers, etc.), there may be other hosts and/or applications available on the DMH network that would not require a proxied connection for valid access. The list of services available is quite extensive, and each would need to be appropriately justified, just as if the user were based in a physical DMH office.